NIS 2 Compliance Blueprint: A Step-by-Step Guide to Strengthen Cybersecurity

To comply with the NIS 2 Directive (Directive (EU) 2022/2555), companies should consider undertaking the following actions:

1. Determine Applicability:
    - Assess if your organization falls within the sectors and services outlined in Annexes I and II of the NIS 2 Directive and meets the relevant financial thresholds.
2. Implement Risk Management Measures:
    - Develop and enforce policies for risk analysis and information system security.
    - Establish incident handling procedures, including prevention, detection, and response.
    - Ensure business continuity through backup management and disaster recovery plans.
    - Secure supply chain management and relationships with service providers.
    - Adopt measures for assessing the effectiveness of cybersecurity risk management.
3. Establish Incident Reporting Procedures:
    - Set up processes to detect, report, and address significant incidents.
    - Notify the relevant Computer Security Incident Response Team (CSIRT) or competent authority without undue delay.
4. Appoint a Security Officer:
    - Designate a responsible person for overseeing compliance with NIS 2 requirements.
5. Conduct Regular Training and Awareness Programs:
    - Provide ongoing cybersecurity training for staff to ensure awareness and preparedness.
6. Engage in Information Sharing:
    - Participate in information-sharing networks to stay informed about threats and best practices.
7. Prepare for Supervision and Enforcement:
    - Be ready for potential audits and assessments by national authorities.
    - Maintain documentation of all cybersecurity measures and incident reports.

By following this checklist, companies can align with the NIS 2 Directive's requirements and enhance their cybersecurity posture.